Privacy Provision of the Gramm Leach Bliley Act and Recent Privacy Developments

The 2nd Annual Spring Meeting

OF THE **BUSINESS LAW SECTION**
AND THE **INTELLECTUAL PROPERTY SECTION**
OF THE STATE BAR OF CALIFORNIA
APRIL 27-29, 2001, HILTON LA JOLLA, TORREY PINES

Deborah S. Thoren-Peden

I. OVERVIEW OF THE GRAMM LEACH BLILEY ACT'S PRIVACY PROVISIONS

On January 26, 2001 the FDIC released a Privacy Rule Handbook (PR-7-2001) to help financial institutions comply with the new privacy regulations contained in the Gramm Leach Bliley Act (15 USC 6801 et. seq.). The Handbook does an excellent job of explaining the basic privacy rules, provides suggestions for implementation, and recommends activities to monitor and maintain compliance on an ongoing basis.

Section One of the handbook contains the overview of the regulation. It states that:

1. All financial institutions must develop both initial and annual privacy notices that describe in general terms the financial institution's information sharing practices for consumers. The initial privacy notices must be given out by July 1, 2001, and since consumer customers must be given a "reasonable opportunity to opt out" of at least 30 days, this means that notices being mailed to customers must be sent by June 1, 2001.

2. Financial institutions that share nonpublic personal information about consumers with nonaffiliated third parties (outside of certain exceptions) are required to give consumers an opt out notice and a reasonable period of time to opt out. (Sharing such information with affiliated parties is covered by the Fair Credit Reporting Act described in further detail below.)

3. The exceptions to the opt out requirement including sharing with a nonaffiliated party in order to process or service transactions requested or authorized by a consumer; market the financial institution's own financial products or services; market financial products and services offered pursuant to a joint marketing agreement with another financial institution; protect against fraud or unauthorized transactions; respond to legal process; or to comply with applicable legal requirements.

4. In general, financial institutions are prohibited from disclosing an account number or access code for a credit card, deposit or a transaction account to a nonaffiliated third party for its use in marketing. A financial institution may share account numbers in order to market its own products, so long as the financial institution's service provider for the marketing is not authorized to directly initiate charges to the accounts. In addition, a financial institution may disclose account numbers to a participant in a private label or affinity credit card program if the participant has been identified to the customer. This prohibition does not include a number or code in an encrypted form so long as the financial institution does not provide a means to decode the number.

5. There are limits on reuse and redisclosure of information received from a nonaffiliated financial institution or disclosed to a nonaffiliated financial institution.

6. State law providing greater consumer protections will supercede the GLB.

7. The privacy notices must contain, as applicable, the categories of information collected; the categories of information disclosed; the categories of affiliates and nonaffiliates to whom nonpublic personal information is disclosed; information sharing practices about former customers; the categories of information disclosed under the service provider/joint marketing exception; the consumer's right to opt out; Fair Credit Reporting Act disclosures; and disclosures about the confidentiality and security of information. The regulations provide "model" disclosures

that can be used as guidance; however the privacy notice given must reflect the financial institution's actual practices.

The Handbook states that each financial institution needs to create a comprehensive inventory of its information collection and information sharing practices. This should include the review of all applications and forms used to collect information about consumers; all relevant marketing practices; all vendor contracts; electronic banking and Internet activities; fee income accounts; and record retention policies.

II. YOU MAY BE A "FINANCIAL SERVICES PROVIDER" UNDER GLB, BUT DON'T KNOW IT

The GLB's privacy provisions apply to any entity that falls within its definition of "financial institution." The term "financial institution" is defined very broadly and covers many types of businesses that normally would never consider themselves to be a "financial institution." Accordingly, there are a number of businesses and other entities that appear to be unaware that they must comply with the GLB's provisions.

The Federal Trade Commission ("FTC"), which has regulatory oversight of non-bank businesses that are covered by the GLB regulations, provided guidance on the types of business that are covered by the GLB in the final rules it issued on May 24, 2000 (Federal Register, Vol. 65, No. 101, page 33646-33689). A financial institution includes any institution the business of which is engaged in financial activities as described in 4(k) of the Bank Holding Company Act of 1956" (12 USC 1843(k). The covered financial activities include both traditional and non-traditional financial activities, including those "found to be either closely related to banking, or usual in connection with the transaction of banking or other financial institutions abroad. (Fed. Reg. Page 33647. The Bank Holding Company Act, Section 4(k)(4)(A-E) deems the following activities to be "financial in nature:

· Lending, exchanging, transferring, investing for others or safeguarding money or securities;

· Insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death, or providing and issuing annuities, and acting as principal, agent, or broker for purposes of the foregoing, in any State.

- Providing financial, investment, or economic advisory services, including advising an investment company.
- Issuing or selling instruments representing interests in pools of assets permissible for a bank to hold directly.
- Underwriting, dealing in, or making a market in securities."

In addition, the following activities have also been found to be closely related to banking:

- Brokering or servicing loans;
- Leasing real or personal property (or acting as agent, broker, or advisor in such leasing) without operating, maintaining or repairing the property;
- Appraising real or personal property;
- Check guaranty, collection agency, credit bureau and real estate settlement services;
- Providing financial or investment advisory activities including tax planning, tax preparation, and instruction on individual financial management;
- Management consulting and counseling activities (including providing financial career counseling);
- Providing courier services for banking instruments;
- Printing and selling checks and related documents;
- Community development or advisory activities;
- Selling money orders, savings bonds or traveler's checks; and
- Providing financial data processing and transmission services, facilities (including hardware, software, documentation, or operating personnel), databases, advice, or access to these by technological means.

Activities that have been found to be "usual in connection with the transaction of banking or other financial

operations abroad" include:

· Leasing real or personal property (or acting as agent, broker or advisor in such leasing) where the lease is functionally equivalent to an extension of credit;

- Acting as a fiduciary;
- Providing investment, financial or economic advisory services; and
- Operating a travel agency in connection with financial services (e.g., the agency offers credit, investment or insurance products or services).

Entities that come within the definition of "financial institution" will be subject to the GLB only if they have consumers or establish consumer relationships. Those that deal only with businesses are exempt. For example, a real estate appraiser who performs services only for banks, but does not provide services to individuals would not be covered. Please note, however, that if the business is a sole proprietorship, then consideration needs to be given to whether a transaction is being done for a business purpose or for a personal, family or household purpose, and if the latter, then the regulation would apply.

Moreover, the FTC has stated in its final rules that a business that is a "financial institution" is covered by the act "only if the entity is significantly engaged" in activities that are financial in nature. (Federal Register, page 33654). The FTC has provided the following examples of entities that are not "significantly engaged in financial activities":

> 1. A retailer that merely accepts payments in the form of cash, checks or credit cards that it did not issue;
>
> 2. A merchant that allows an individual to run a tab;
>
> 3. A grocery store that allows individuals to cash a check or write a check for an amount more than the amount of the groceries;
>
> 4. A retailer who allows lay away or deferred payment plans or payment by means of credit cards issued by others. (16 CFR Part 313.3(k)(4)

A business' status as a financial institution would not cause every product or service offered by the business to be a financial product or service. For example, a retailer that issues its own credit card directly to consumers provides a financial service to consumers who use the card, but when it sells merchandise it is providing a nonfinancial product or service.

Given the breadth of the definition of "financial institution" it is not surprising that many businesses that never considered themselves to be engaged in financial services in fact are subject to the GLB.

III. CONTACTUAL LANGUAGE TO INCLUDE IN CONTRACTS WITH THIRD PARTIES

The GLB requires financial institutions to include in their contracts with third party service providers and joint marketers language that prohibits the third party from disclosing or using any consumer nonpublic personal information that the third party received from the financial institution in any manner other than to carry out the purposes of the contract in the ordinary course of business. Suggested below is language that can be incorporated into such third party contracts:

> A. Confidentiality: [Insert name of Vendor] ("Vendor") acknowledges that in performing services hereunder, Vendor will have access to, and Bank will provide Vendor with information and/or documentation about Bank's customer which constitutes confidential information ("Confidential Information"). Confidential Information includes, but is not limited to any information about Bank's customers or potential customers, regardless of whether it is personally identifiable or anonymous information. Vendor agrees now and at all times in the future that all such Confidential Information shall be held in strict confidence and disclosed only to those employees whose duties reasonably require access to such information. Vendor may use such Confidential Information only in connection with its performance under this Agreement. Vendor shall establish and maintain

commercially reasonable policies and procedures to ensure compliance with this section. Vendor agrees that such policies and procedures will be consistent with the Bank's customer information security program. Vendor shall protect such Confidential Information in accordance with commercially reasonable standards and at a minimum using the same degree of care, but no less than a reasonable degree of care, to prevent the unauthorized use, disclosure or duplication of such Confidential Information as Vendor uses to protect its own confidential information. Confidential Information shall be returned to Bank or destroyed upon Bank's request once the services contemplated by this Agreement have been completed or upon termination of this Agreement. Vendor acknowledges that the unauthorized use, disclosure or duplication of any such Confidential Information is likely to cause irreparable injury to Bank and/or to Bank's customers for which Bank and/or Bank's customers will have no adequate remedy at law. Accordingly, Vendor hereby consents to the entry of injunctive relief against it to prevent or remedy any breach of the confidentiality obligation described herein without Bank being required to post bond. Further, Vendor agrees that any violation of this section by Vendor shall be a material breach of this Agreement and shall entitle Bank to immediately terminate this Agreement without penalty upon notice to Vendor. Vendor agrees to permit Bank and Bank's regulators to audit Vendor's compliance with this section, and with all applicable laws and regulations, during regular business hours upon reasonable notice to Vendor. The provisions of this section shall survive any termination of this Agreement.

IV. FAIR CREDIT REPORTING ACT ISSUES

On December 22, 2000 the Federal Trade Commission issued Proposed Interpretations of the sections of the Fair Credit Reporting Act that permit financial institutions and companies to communicate customer information to affiliates without incurring the obligations of consumer reporting agencies. These FCRA regulations must be considered and complied with in addition to the GLB privacy provisions. Every financial institution must be aware that even if its sharing of nonpublic personal information qualifies for an exemption under GLB, it may still be deemed to be a consumer reporting agency under FCRA if the information shared involves non-experiential or non-transactional information.

By way of background, the FCRA provides that if a financial institution or business regularly passes on information in its files about a consumer, other than information solely about its transactions or experiences with a consumer, then it may be deemed to be a "consumer reporting agency." A "consumer reporting agency" includes any person or business of any type which, for fees or for free, "regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties", and which uses any means of interstate commerce to prepare or furnish such reports. (15 USC 1681 Section 603(f). A "consumer report" includes any "written, oral or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for: (A) credit or insurance to be used primarily for personal, family or household purposes; (B) employment purposes;" or (C) any other permissible purpose for furnishing such reports, which includes, but is not limited to a "legitimate business need for the information in connection with a business transaction that is initiated by the consumer or to review an account to determine whether the consumer continues to meet the terms of the account. (15 USC 161 Section 603(d) and Section 604).

A financial institution or business is allowed to relate information solely about its transactions or experiences with a consumer without becoming a consumer reporting agency. For example, a financial institution may disclose that a consumer had a history of delinquency and could give other information about the status of any loans or deposits that the consumer has with it. However, a financial institution or business may not regularly give out information contained in credit or other applications that bear on the any of the following characteristics: creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living to the extent such information is neither transaction nor experiential in nature. In addition, a financial institution or business may not regularly give out information obtained in reports from consumer reporting agencies or any other non-experiential or non-transactional information obtained from a third party. An entity that obtains information as a "user" can become a consumer reporting agency if it subsequently conveys the information to another entity, even if the other entity is its affiliate. (FCRA, Questions

and Answers, Q 16, 17 and 18).

The FCRA does allow sharing non-experiential or non-transactional information with affiliates, so long as the consumer has been given a clear and conspicuous right to opt out. This exception arises from the FCRA's definition of "consumer report" which excludes any:

- report containing information solely as to transactions or experiences between the consumer and the person making the report;
- communication of that information among persons related by common ownership or affiliated by corporate control; or
- communication of other information [i.e., non-experiential or non-transactional] among persons related by common ownership or affiliated by corporate control, if it is clearly and conspicuously disclosed to the consumer that the information may be communicated among such persons and the consumer is given the opportunity, before the time that the information is initially communicated, to direct that such information not be communicated among such persons." (15 USC 1681, Section 603(d)(2)(A).

Accordingly, a financial institution or business can avoid being deemed to be a consumer reporting agency if it gives its customers an opt out notice regarding its sharing of non-experiential and non-transactional information with its affiliates, and then refrains from sharing such information for any consumer customers who choose to exercise their opt out rights. (Most businesses and banks assiduously try to avoid being deemed to be a consumer reporting agency as consumer reporting agencies are allowed to make reports only to parties with permissible purposes, may not report negative information after a set period of time, must maintain procedures to ensure accuracy of reports, must make file disclosures to consumers, and must reinvestigate disputes using specified procedures.)

Congress made it clear in the GLB that its privacy regulations do not modify, limit or supercede the operations of the FCRA, (although the GLB does require that the FCRA opt out notice be included in the initial and annual privacy notice provided to customers and consumers). Accordingly, both the GLB privacy regulations and the FCRA can apply to financial institution's or business' disclosures of certain consumer information.

The proposed FCRA implementation rules would require the opt out notice to accurately explain (1) the categories of opt out information about the consumer that the company communicates to others; (2) the categories of affiliates to which the company communicates the information, (3) the consumer's ability to opt out, and (4) a reasonable means of opt out. In addition to going into depth regarding each of these items, the proposed rules provide a sample opt out notice.

The regulatory agencies have received numerous comments from financial institutions, trade associations and others complaining that these proposed regulations are problematic in terms of the GLB privacy notices. Among other things, these regulations would require many financial institutions to provide very different privacy notices to their consumers than the ones that they have provided or are about to provide under the GLB. In addition, many are concerned that even though a financial institution may qualify to share information under one of the exceptions in the GLB, they may be deemed to be a consumer reporting agency. Due to the issues raised in these comments, and the need to work with the banking regulatory agencies on the various issues, the FTC allegedly has decided not to issue final rules until after July 1, 2001, and may even issue another set of proposed rules before issuing final rules. During the interim, however, businesses and financial institutions are strongly advised not to share non-experiential or non-transactional information with third parties where such third parties might use the information for one of the purposes described above in the definition of "consumer report," especially in light of the concerns that various attorney generals throughout the country may start to bring actions against entities that violate the FCRA.

V. ACCOUNT AGGREGATION SERVICES

On February 28, 2001 the OCC issued a bulletin discussing the risks of financial institution-provided account aggregation services. (OCC 2001-12) The bulletin recommends control mechanisms financial institutions should consider when they offer aggregation services.

An aggregation service is one that gathers information from many web sites and presents the information in a

consolidated format to a customer. The information gathered may include publicly available information and personal account information, such as credit card, brokerage and banking data. The bulletin advises financial institutions that offer aggregation services to be careful to ensure their privacy policies accurately reflect the categories of information that collected and disclosed in its aggregator role, as they may be different from the type of information the bank collects and discloses in connection with its usual banking products and services. It may even be appropriate for a financial institution offering such aggregation services to provide separate notices to its aggregation customers.

The bulletin also warns financial institutions about the implications of the FCRA as the sharing of information with affiliates or other parties that does not relate to the financial institution's own transactions and experiences may result in the financial institution being deemed to be a consumer reporting agency. The bulletin notes that if an aggregator discloses to nonaffiliated third parties consumer information it compiled from other sources, such as deposit account information, then it may be considered a consumer reporting agency even though it has received the consumer's consent for such disclosures. Any financial institution or other entity that is considering or currently offering aggregation services should obtain and read this bulletin.

VI. NEW PRIVACY LEGISLATION AND REGULATION

A. International:

Canada has enacted a new privacy law, effective January 2001 that applies to the collection, use and disclosure of any personally identifiable information. (The Personal Information and Electronic Documents Act, Statues of Canada 2000, Chapter 5, Elizabeth II, April 13, 2000). The law, which is similar in scope to the European Union Directive on Data Protection (adopted October 24, 1995), requires notice and consent before the collection and sharing of virtually any type of personally identifiable data.

Australia and Argentina: Both Australia and Argentina have also enacted laws, very similar in scope to the Canadian law. (The Privacy Amendment. Private Sector, Bill 2000, Commonwealth of Australia; Personal Data Protection Act, October 4, 2000, Act 25,326 of the Argentine Nation in Congress).

Any financial institution that operates internationally and shares personally identifiable information across borders for purposes other than processing a customer's transaction may be subject to these international laws, and needs to address the attendant compliance issues.

B. Federal:

On the federal front, other than the GLB, the most significant development in privacy was the issuance of new medical privacy rules by the Department of Health and Human Services, on December 28, 2001. The rules, which require patient's consent for virtually any type of disclosure of medical information, are extremely complex, and many believe are too cumbersome work. They appear to apply to many financial institutions and businesses that offer health plans that provide medical care that qualify under ERISA. The Bush administration has temporarily delayed the effective date of the new regulation and is in the process of reconsidering the rules.

C. State:

SB 129: An Office of Privacy Protection was created within the Department of Consumer Affairs. The office has no enforcement or substantive rulemaking authority, but its mission is to provide consumer education, recommendations on fair information practices, be a resource center for identity theft prevention and facilitate mediation and arbitration of privacy disputes.

SB 1724: Privacy of Tax Return Information Held by Lenders. The law prohibits lenders who require tax returns as part of loan documentation from disclosing information contained in a tax return unless the lender has a specific authorization from the taxpayer to do so. Such information may be disclosed to third parties for operational purposes.

AB 2246: Proper Disposal of Business Records. All California business are now required to take "all reasonable steps" to destroy or arrange for the destruction of all customer records containing personal information that are no longer to be kept by the business. The records or documents can be destroyed by shredding, erasing or otherwise making the records unreadable or undecipherable.

AB 2797: Ban on Sharing Medical Information with Credit Grantors. Life, disability and health insurance underwriters or sellers are prohibited from sharing personally identifiable health, medical or genetic information with credit grantors, regardless of whether they are affiliated or unaffiliated.

AB 1862: Identity Theft Victim Database: The Department of Justice is required to establish a database containing the names of identity theft victims which can be accessed by law enforcement agencies, victims and other individuals and agencies authorized by victims.

AB 1897: Remedies for Victims of Identity Theft: Anyone who is (or reasonably believes he is) a victim of identity theft may now initiate a law enforcement investigation and petition for an expedited judicial determination of innocence if their name or personal information has been associated with criminal activity.

VII. PROPOSED LEGISLATION

A. Federal:

Numerous bills have already been introduced into Congress related to privacy and the Internet (they have been averaging one per day since Congress convened). Described below are some of the bills of particular interest:

S. 450: The Financial Information Privacy Protection Act of 2001 would allow consumers to opt out of information sharing between affiliated firms and create an opt in right for certain medical and sensitive financial data, such as a person's spending habits. Customers would also have the right to view the information that was shared and have any errors in the information corrected.

S. 451: The Social Security Number Protection Act of 2001 would establish civil and criminal penalties for the sale or purchase of a social security number.

S. 324: The Social Security Privacy Act would prohibit the sale and purchase of social security numbers and amend GLB to promote privacy.

S. 197: The Spyware Control and Privacy Protection Act would protect the privacy of online shoppers and other Internet users whose activities are secretly monitored by "spyware" software.

H.R. 718: The Unsolicited Commercial Electronic Mail Act of 2001 would criminalize the sending of unsolicited commercial email where the sender has knowledge that the information identifying the sender is false or inaccurate. It would also require the inclusion of a return address to be used to advise the sender to send no further emails to the address, and prohibit transmission of such emails after receipt of such an opt out.

H.R. 347: The Consumer Online Privacy and Disclosure Act would require web sites to obtain consumer customer permission before tracking their online movements with cookies. The legislation would also require the Federal Trade Commission to create standards that companies would be forced to meet in posting their privacy policies. In addition, bankrupt e-commerce companies would be prevented from selling their customer transaction lists and personal information to pay off creditors.

H.R. 237: The Consumer Internet Privacy Enhancement Act would make it unlawful for a

commercial website operation to collect personally identifiable information online from a user unless it has provided notice to the user and an opportunity to opt out of its use for marketing purposes or from having it disclosed to third parties where the information collected is not related to the provision of the products or services provided by the website.

B. State:

AB 21: The Financial Privacy Act would require specified disclosures be given to consumers before collecting or sharing nonpublic personal information with affiliates or with nonaffiliated parties. It would impose both initial and annual opt out requirements.

AB 109: The Elder and Dependent Adult Abuse Act would require financial institutions to report all types of suspected elder abuse, including financial, physical and emotional abuse, to local law enforcement or protective services. There is a limited immunity for financial institutions that report such information in "good faith."

AB 203: The Consumers' Financial Privacy Act would require the consumer's prior written consent before disclosing or making unrelated use of personally identifiable information. "Unrelated use" would include any use other than to effect, administer or enforce a transaction or that exceeds the stated purpose for which the consumer had given his consent.

SB 17: This bill, which is described as addressing unsolicited and unwanted telephone solicitations, would empower an agency (to be defined) to maintain a "do not call" list. Telephone subscribers would be able to have their telephone numbers placed on a list, and could designate entities from which they will accept telephonic solicitations. Telephone solicitors would be able to obtain a copy of the list for a fee.

SB 125: This bill, which is described as an identity theft law, would provide that where someone's identity has been used to open an account or obtain a loan, credit or charge card, the person whose identity was stolen would be entitled to obtain information related to the transaction from the entity with which the transaction was conducted.

SB 168: This bill, which is described as a personal information, confidentiality and identity theft law, would allow a consumer, through a toll-free number, to put a credit bureau on a "security alert" and request a "security freeze" on releasing any information in their file. The bill would also ban use of a social security number to obtain a product or service, with limited exceptions.

SB 169: This bill, which is described as addressing credit, confidentiality and identity theft, would entitle a victim of identity theft to obtain a copy of an application that was used by an unauthorized person to obtain a loan, credit or charge card.

VIII. IDENTITY THEFT

Identity theft is one of the fastest growing types of crime, with approximately 500,000 cases each year, at an average cost of $17,000 per person, according to statistics compiled by the Federal Trade Commission. Identity theft involves the theft of another's self or identity via the use of personally identifiable information that has either been stolen or obtained without appropriate authorization. People from every walk of life are impacted, and even Tiger Woods has had his identity used to fraudulently purchase goods. Approximately 54% of identity theft involve the fraudulent or unauthorized use of credit cards. (ABA Banking Journal, "Identity Theft" January 2001)

Identity theft crimes are usually committed by "pros" who steal information from the Internet, steal mail or wallets, dive in dumpsters or pose as prospective employers or as the customer himself in order to obtain the information they seek. There are also waiters and retail outlet clerks who use scanning devices to lift the relevant information from legitimate credit card transactions. Moreover, there are information brokers who are willing to sell data to anyone without asking meaningful questions about the legitimacy of the request, as well as telemarketing scams. Competent identity thieves can take an address or a social security number and use it to obtain a relatively complete picture of the financial history of an individual.

There is an active debate on whether additional laws should be passed to require banks to do more to protect customers against identity theft. Partially in response to this debate, the Gramm Leach Bliley Act ("GLB") required the banking agencies to establish appropriate standards for safeguarding customer records and information. On February 1, 2001 the agencies published Interagency Guidelines Establishing Standards for Safeguarding Customer Information, which require banks to implement comprehensive customer information security programs by July 1, 2001. The GLB also made it a federal crime to obtain private consumer information through fraudulent means.

The impact of identity theft on an individual can be significant. Because of the limitations on consumer liability imposed by the Truth in Lending Act and the Electronic Funds Transfer Act, in most cases the maximum liability of a consumer for unauthorized charges is $50, and many lenders waive this amount for their customers. However, victim's credit cards and credit lines can be charged to the maximum levels, bank accounts and overdraft lines can be emptied, new accounts can be opened (with the bank statements being sent to addresses provided by the thieves), and credit ratings and histories can be ruined. Victims have to spend a great deal of time contacting the police, filing a report, contacting their financial institutions and credit card issuers, and the consumer reporting agencies in an effort to try to clean up the havoc wreaked by the identity theft.

Banks and bankers are and have been actively engaged in trying to protect bank customers from identity theft for a number of years. The American Bankers Association ("ABA") has developed an Identity Theft Prevention and Resolution kit, which can be obtained by going to www.aba.com; or calling 1-800 BANKERS.

There are certain actions that individuals can take to help protect themselves, including but not limited to the following:

- Do not transmit your credit or debit card number or checking account information over the Internet unless the website has appropriate security measures.
- Never divulge your social security number, credit or debit card number, or checking account information to anyone unless you are absolutely certain that the information is being requested for a legitimate reason and you are certain of the identity of the party who is requesting the information.
- Do not include your social security number on your checks.
- In general, you should never provide your credit or debit card or checking account information over the phone in response to someone who calls you.
- Protect your Personal Identification Numbers and passwords or passcodes carefully.
- Destroy your credit and debit card receipts, bank statements and credit card offers after they are no longer needed for tax or other purposes.
- Mail bills from the U.S. post box or post office; bills mailed from your mailbox may be stolen.
- Carefully review your checking and credit card statements each month to ensure that all transactions are authorized and correct.
- In the event that any transactions appear to be unauthorized or erroneous, immediately report your suspicion to the bank that sent the statement or the credit card issuer.
- Review your consumer credit report on a periodic basis (at least once per year) to ensure the information is correct.
- Immediately respond to any inquiry from your bank regarding the legitimacy of a transaction.

If you become a victim of identity theft contact your bank and credit and debit card issuers immediately and file a police report. You should also contact the fraud unit of each of the major credit reporting agencies, and, if appropriate, place a victim statement in your credit report. The phone numbers of the fraud units at the agencies are: Equifax (800) 525-6285; Experian (888) 397-3742 and Trans Union (800) 680-7289.

IX. WHAT CAN BANKS DO TO HELP?

Have appropriate consumer information systems.

A. Customer Information Security Program

In addition to the GLB's privacy notice and procedure requirements, the GLB requires each financial institution to evaluate the safeguards it has for protecting customer information. In response to this mandate, the banking agencies issued a Joint Final Rule for Security Standards for Safeguarding Customer Information on February 1, 2001. (Federal Register, Vol. 66, No. 22, pages 8616-8641) The Rule describes the standards contained therein as "Guidelines." Under the Guidelines each financial institution must implement a customer information security program by July 1, 2001. Each financial institution has until July 1, 2003 to include certain required contractual provisions in its contracts with service providers.

The information security program must be designed to "ensure the security and confidentiality of customer information; protect against any anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer." Id. At 8640.

1. Developing and Implementing the Information Security Program:

The Guidelines require each financial institution to implement a comprehensive written information security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the financial institution, as well as the nature and scope of its activities

2. Board of Directors Involvement:

The Guidelines require the involvement of the board of directors of each financial institution, or an appropriate committee of the board. The board or board committee must approve the written information security program. The board or board committee must also oversee, on an ongoing basis, the development, implementation and maintenance of the information security program, including assigning specific responsibility for its implementation and review of reports from management.

The board or appropriate board committee is to receive a report on the overall status of the information security program and the financial institution's compliance with the Guidelines on at least an annual basis. The report should discuss material matters related to the program; risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations; management's responses; and recommendations for changes in the information security program.

3. Risk Assessment:

Each financial institution is required to assess its risk by:

- Identifying reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems.
- Assessing the likelihood and potential damage of internal and external threats, in light of the sensitivity of customer information.
- Assessing the sufficiency of its policies, procedures, customer information systems, and other arrangements to control risks.

4. Management and Control of Risk:

Each financial institution's program must be designed to control its identified risks. The following security measures are to be considered by the financial institution,

and where appropriate, adopted:

- "Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who seek to obtain this information through fraudulent means.
- Access restrictions at physical locations containing customer information, such as buildings, computer facilities and record storage facilities to permit access only to authorized individuals.
- Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access.
- Procedures designed to ensure that customer information system modifications are consistent with the information security program.
- Dual control procedures, segregation of duties and employee background checks for employees with responsibilities for or access to customer information.
- Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems.
- Response programs that specify actions [to be taken when the financial institution] suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies.
- Measures to protect against destruction, loss or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures." Id at 8640.

5. Training and Testing:

Each financial institution must train its staff to implement the security program. This would include training them to recognize, respond to and report unauthorized attempts to obtain customer information.

The financial institution must regularly test the key controls, systems and procedures of its information security program. The frequency and nature of such tests should be determined by the financial institution's risk assessment. Appropriate tests should be conducted or reviewed by independent third parties or staff other than those who develop or maintain the security programs. The Guidelines do not prescribe specific tests.

6. Overseeing Service Providers:

Each financial institution needs to perform a risk assessment to determine the risks posed by its service providers. The financial institution is required to exercise appropriate due diligence in selecting service providers, and to require such providers, by contract, to implement appropriate measures designed to meet the objectives of these Guidelines. (The proposed vendor language above would require the vendor to keep the information confidential, to use commercially reasonable security standards, and to maintain standards that meet with the financial institution's information security program. However, depending upon the vendor, there may be situations where the contract's language should be more comprehensive in scope, and require many of the items described in section 4 above.) In addition, where indicated by the risk assessment, the financial institution needs to monitor its service providers to confirm they have satisfied their obligations, including reviewing the service provider's audit reports and test results.

7. Adjusting the Program:

The financial institution must monitor, evaluate and adjust as appropriate, its information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and its own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to customer information systems.

X. VENDOR PRACTICES AND POLICIES

On November 28, 2000 the Federal Financial Institutions Examination Council ("FFIEC") issued guidance on financial institutions' management of risk arising from technology services supplied by outside firms. The guidance made it clear that boards of directors and senior management need to oversee and manage outsourcing relationships, and that each financial institution should have an outsourcing process that includes (a) a risk assessment to identify the institution's needs and requirements; (b) proper due diligence to identify and select a provider; (c) written contracts that clearly outline duties, obligations and responsibilities of the parties involved; and (d) ongoing oversight of outsourcing technology services.

Although the guidance is specific to outsourced technology services, it is extremely useful and should be considered as guidance for any type of outsourcing. The guidance recommends that an outsourcing risk assessment should be done by the bank, considering, among other things, the needs of the bank and its ability to oversee such relationships, the importance of the service to the bank, the needed controls and reporting processes, contingency plans, regulatory requirements, ongoing assessment, and the contractual obligations.

Banks are to perform appropriate due diligence in selecting a service provider. The bank should carefully evaluate the service provider's technical and industry expertise, the operations and controls it uses and its financial condition. The guidance provides numerous factors to consider under each of these categories.

The guidance also recommends that certain contractual provisions should be included in the outsourced arrangements. The contract should clearly describe the rights and responsibilities of the parties to the contract and the scope of service. Performance standards defining minimum service level requirements should be included as well as the remedies in the event the service provider fails to meet these standards. The contract should address the service provider's obligations and responsibilities in terms of security and confidentiality of the institution's resources (such as information and hardware), and prohibit the disclosure of such information unless needed to provide the contracted services. The bank should advise the service provider to assess the applicability of the GLB and FCRA privacy provisions if the service provider is to receive nonpublic personal information. The service provider should be required to promptly and fully disclose any breaches in its security that result in unauthorized intrusions that could materially affect the bank or its customers, and report the effect on the bank and the corrective actions taken.

The contract should address:

- Controls over the service providers' operations, such as its internal controls;
- Compliance;
- Records to be maintained;
- Insurance coverage;
- Access to such records by the bank and bank's regulators and auditors;
- Notification and approval rights regarding material changes to services, systems, controls, key project personnel and new service locations;
- The setting and monitoring of payment processing and extensions of credit on behalf of the bank;
- Identification of the types of reports the bank is entitled to receive, including but not limited to audit reports, financial statements, security, business resumption testing, performance and custom reports, along with the frequency of such reports;

- The service provider's responsibility for backup and record protection;
- The service provider's business resumption and contingency plans;
- Notification and approval requirements related to sub-contracting or multiple provider relationships;
- A complete description of fees and calculations for the services, including development, conversion, recurring services, volume of activity, special requests, maintenance, and ability to change such costs;
- Ownership and license of the data, equipment/hardware, system documentation, system and application software and other intellectual property rights;
- Duration;
- Dispute resolution;
- Indemnification;
- Limitation of liability;
- Terminations rights; and
- Ability to assign.

The guidelines also recommend that management oversees the relationship, and that the degree of oversight will vary depending upon the nature of the services outsourced. It is recommended that the financial institution monitor the ongoing financial conditions and operations of the service provider; assess the quality of the service and the provider's ability to support and enhance the bank's strategic direction on an ongoing basis; monitor contract compliance and the need to revise such contract; and ensure the service provider's business resumption plans and contingency plan testing continue to be sufficient. The guidelines basically provide a checklist of items that should be done and considered in connection with every arrangement entered into with an outside service provider.